REMARKS

In response to the objection to the title of the invention, as set forth in item 3 on page 2 of the Office Action, Applicants have amended the title to clearly indicate the nature of the claimed invention. Accordingly, reconsideration and withdrawal of this ground of objection are respectfully requested.

Claims 1-5 and 7-12 have been rejected under 35 U.S.C. §102(b) as anticipated by Araujo et al (Published U.S. Patent Application No. 2003/0191799 A1). However, for the reasons set forth hereinafter, Applicants respectfully submit that all claims of record in this application distinguish over the cited reference, whether considered separately or in combination. In this regard, Applicants note that they have made minor revisions in the first and third paragraphs of Claim 1, for the purpose of consistent terminology and continuity. However, the latter changes do not alter the scope of the claim.

BACKGROUND

The present invention relates to an arrangement which avoids sensitive data being left on a user terminal after a network browsing session. This is important in situations such as internet cafés, where one person may use a terminal and enter sensitive data (for example the entry of passwords and credit card numbers). A second user may later be assigned to the same terminal, and if the first user's sensitive data are stored on the terminal, it is possible that the latter user may be able to discover and misuse the sensitive data.

The present invention provides a solution to this problem by providing a remotely-accessible web browsing software, which a user may know and trust not to store sensitive data on the user terminal. In particular, the user may use the <u>terminal's standard network browser</u> to access a remote server to <u>download the trusted web browsing software</u>, and use the trusted web browsing software to carry out transactions which involve the entry of sensitive data. When the user has finished using the terminal, he closes the trusted web browsing software and disconnects from the remote server. As a result, no sensitive data remain on the terminal, and any later user would be able to discover only that the first user accessed the remote server and downloaded a web browsing software.

Araujo et al provides a different solution to a very different problem: it provides a way to securely connect a PC to a server for secure data access across different applications using a web browser's built in secure socket layer (SSL) as a lightweight virtual private network (VPN) without the 'overhead' of IPsec. Nowhere does it mention the security of the local terminal with regard to caching of files and nowhere does it mention general web browsing: Araujo et al is a point to point solution.

In particular, Araujo et al addresses the problem of users who are remote from their office, but wish to access a range of stored data and applications that are not present on their terminal which is available to them at the remote location. The terminal may be a desktop PC at a remote location, or a portable computer of some sort. Rather than having to install and maintain a full range of desired applications on each computer, and to ensure that all data are synchronized between the various computers which the user may access, Araujo et al provides a networked solution in which the user accesses applications and data through a web browsing software that is resident on the local terminal. That is, the user uses the terminal's standard web browsing software to contact to a remote server. The user may then download the required application software and remotely interact with data stored on a remote server. The user will be able to access data and use applications as if his terminal were locally connected to an office network.

Araujo et al is unconcerned with the issue of whether entered data are subsequently stored on the user's terminal or are accessible to subsequent users of the same terminal, since in the applications envisioned by Araujo et al, the terminal is personal to the user. Araujo et al allows desired application software to be downloaded to a user's terminal through use of a standard browser. It does not provide a trusted web browsing software which is remotely accessible for download and use on non-secure terminals, as in the present invention, but rather provides a virtual-office application for remote workers.

See, for example, Paragraphs [0029] and [0030]; Paragraph [0031]; Paragraph [0060]; and Paragraph [0064] (lines 21-28). While Araujo et al discloses remote access to applications, and the downloading of HTML files for graphical display purposes, (Paragraph [0064] lines 1-28), it is important to note that, in particular, no web browser software is downloaded and used at the terminal. Rather the system uses the web browser 15 (Fig. 1) that is already present on the user terminal for all browser activity. See Paragraphs [0061] and [0064] lines 27-28.

RESPONSE TO CLAIM REJECTIONS

CLAIM 1:

Araujo et al contains no provision for "transmitting a request for web browsing software stored on the server to be downloaded to a terminal". Moreover, it also fails to teach or suggest any provision for "receiving web browsing software at the terminal", or "using the web browsing software which has been downloaded to the terminal to communicate from the terminal over the public network". Rather, as noted previously, in Araujo et al, no web browsing software is downloaded. All web browsing via the terminal in question is performed using the web browser 15 which is resident on the terminal itself, thereby leaving open the possibility of storing sensitive personal information, which is eliminated by the present application.

Finally, Araujo et al also contains no teaching that downloaded web browsing software (of which there is none in Araujo et al) is configured such that user input data which is input to the web browsing software by a terminal user, or data which are received from the network at the terminal by the web browsing software, are transmitted to the network or presented to the user "without storing a record of the data at the terminal". In fact, given the software and hardware configuration disclosed in Araujo et al, there is no provision which would prevent such storage. Accordingly, a subsequent user of the terminal in question could obtain access to the former user's personal information, since it is stored on the terminal.

Claims 2-5 and 7-12 are allowable due to their dependency on Claim 1. However, Applicants offer the following comments regarding those claims.

CLAIM 2:

In the passage referred to in the Office Action, Araujo et al teaches that a Java applet is used to encode user input data, such as mouse clicks and keystrokes, into AIP protocol, and to pass control information into the SEP of Araujo et al. Applicants respectfully submit, however, that this does not indicate or suggest that a web software embodied as a Java applet is involved, or provided, in any way.

CLAIM 4:

Araujo et al discloses that software is downloaded by and runs within a browser (reference numeral 15 in Fig. 1), but not that the downloaded software is itself a web browsing software.

CLAIM 5:

Insofar as Applicants can determine, Araujo et al discloses no "further browsing software".

CLAIM 7:

Applicants submit that nothing in Fig. 2 suggests that anything is arranged to communicate "with the public data network via a web browser application running on a remote server".

CLAIM 8:

Applicants are unable to identify the subject matter referred to in Araujo et al, since Araujo et al is not arranged by numbered columns and lines.

CLAIMS 9-10:

Araujo et al does not disclose or suggest that no record of input data is stored at the terminal, or that data provided to the user is not stored on the terminal. As discussed at length in the present application, it is a standard feature of virtually all computers that copies of such data will be stored. Accordingly, in the absence of any indication to the contrary, the arrangement of Araujo et al would include the local storage of input and requested data. Moreover, Araujo et al contains no teaching of how to avoid such storage.

In light of the foregoing remarks, this application should be in condition for allowance, and early passage of this case to issue is respectfully requested. If there are any questions regarding this amendment or the application in general, a telephone call to the undersigned would be appreciated since this should expedite the prosecution of the application for all concerned.

If necessary to effect a timely response, this paper should be considered as a petition for an Extension of Time sufficient to effect a timely response, and please charge any deficiency in fees or credit any overpayments to Deposit Account No. 05-1323 (Docket #038819.53225US).

Respectfully submitted,

Gary R Edwards

Gary R. Edwards
Registration No. 31,824

CROWELL & MORING LLP
Intellectual Property Group
P.O. Box 14300
Washington, DC 20044-4300
Telephone No.: (202) 624-2500
Facsimile No.: (202) 628-8844
GRE:kms
2934445_1